

This site uses cookies. By continuing to browse this site you are agreeing to our use of cookies. [Find out more.](#)X



- [SC US](#)
- [SC UK](#)

[Show Search Bar](#)

- [News](#) ▼
 - [Features](#)
 - [Executive Insight](#)
 - [The SC Blog](#)
 - [Business & Finance](#)
 - [Cyber-security events calendar](#)
- [Cyber-crime](#) ▼
 - [Ransomware](#)
 - [Data breaches](#)
 - [APTs/Cyber-espionage](#)
 - [Malware](#)
 - [Phishing](#)
 - [Insider threats](#)
- [Network Security](#) ▼
 - [Mobile security](#)
 - [Cloud security](#)
 - [Privacy & Compliance](#)
 - [Vulnerabilities](#)
 - [IoT](#)
 - [Email security](#)
- [Products](#) ▼
 - [Group Tests](#)
 - [SC Buyer's Guide 2017](#)
- [Video](#)
- [Events](#) ▼
 - [SC Congress London](#)
 - [Editorial Roundtable Series](#)
 - [SC Awards Europe](#)
- [Whitepapers](#)
- [Webcasts](#)

- [Log in](#)
- ●
- [Register](#)

[The Cyber-Security source](#)
[by Rene Millman](#)

January 17, 2018

Cryptocurrency miners target web servers with malware

- [f](#)
- [t](#)
- [in](#)
- [G+](#)
- [g](#)
- [p](#)
- [d](#)

RubyMiner malware plants XMRig on vulnerable systems. Security researchers have discovered malware aimed at Linux and Windows servers running to mine cryptocurrency.



RubyMiner malware plants XMRig on vulnerable systems. Security researchers have discovered malware aimed at Linux and Windows servers running to mine cryptocurrency.

According to researchers at Check Point, attackers have used malware called RubyMiner to infect systems with a cryptocurrency miner called XMRig.

Researchers said in a [blog post](#) that over a 24-hour period last week, hackers attempted to compromise 30 percent of networks worldwide in order to find vulnerable web servers in order to mobilise them to their mining pool. It said that among the top countries targeted are the United States, Germany, United Kingdom, Norway and Sweden, though no country has gone unscathed.

Security firm Certego also noticed a huge spike in attacks as well. It said in a [blog post](#) that the exploit has been trying to leverage a fairly old CVE (CVE-2013-0156) that allows remote code execution.

According to Check Point, the attacker attempts to use multiple web server vulnerabilities to inject the malicious code onto the vulnerable machines. "Among the targeted servers we found attacks on PHP,

Microsoft IIS, and Ruby on Rails,” they said.

Check Point researchers said that the hacker also made use of known vulnerabilities within Ruby on Rails and Microsoft IIS. The Ruby on Rails base64 encoded attack vector exploits CVE-2013-0156.

The attacker sends a base64 encoded payload inside a POST request in the hope that the ruby interpreter configured on the server will execute it.

“This is a very simple bash script that adds a new entry in the crontab of the host. The cronjob is executed once per hour (notice the number 1: it means every first minute of every hour) and it downloads the file robots.txt via wget. The file is piped through bash, so most probably it's a text file containing a shell script,” said researchers at Certego.

Check Point researchers said that it is interesting to note that the scheduler isn't just being told to run the mining process every hour, it is being told to run the whole process, which includes downloading the file from the server.

“This is possibly to allow the attacker to initiate an immediate kill switch for the miner bot. If the attacker would like to end the process on the infected machines, all that needs to be done is modify the robots.txt file on the compromised webserver to be inactive. Within a minute, all the machines re-downloading the file will be receiving files without the cryptominers,” said Check Point researchers.

Check Point said that one of the domains used in this attack, lochjol.com, was seen being used in another attack back in 2013. The previous attack also leveraged the vulnerability in Ruby on Rails, and shares some common features with the current attack

“Nonetheless, we cannot determine the connection between the two, and, even if they share a common attacker, their purposes seem to be different,” said researchers. “In 2018, as in 2017, we continue to see blitz campaigns, leveraging unpatched vulnerabilities in many networks. This attack, like its predecessors, could have been prevented by simply patching old servers and deploying relevant security measures.

Javvad Malik, security advocate at AlienVault, told SC Media UK that as cryptocurrencies gain popularity and value, they become a more attractive target to cyber-criminals.

“Due to the fact that more and more variants emerge frequently, businesses should keep systems updated where possible, and invest in threat detection and response controls that can detect where malicious techniques are being used to mine cryptocurrencies,” he said.

Andy Norton, director of threat intelligence at Lastline, told SC Media UK that Monero is taking over as the “bad boy” of cryptocurrencies due to its fungible nature and CPU friendly algorithm.

“Mining payloads are becoming much more prevalent,” he said. “100 percent of internet connected networks experience compromise attempts on a daily basis. Best practice guidance on protecting infrastructure remains unchanged.”



- 

Topics:

- [Cryptocurrency](#)
- [Linux](#)
- [Malware](#)
- [Mining](#)
- [Research](#)
- [Security](#)
- [Servers](#)
- [Windows](#)

0 Comments

SC Media UK

 Login ▾

 Recommend

 Share

Sort by Newest ▾



Start the discussion...

LOG IN WITH

OR SIGN UP WITH DISQUS 

Name

Be the first to comment.

ALSO ON SC MEDIA UK

Security issue found in the AMD's Platform Security Processor

1 comment • 2 months ago



k_ — Nonsense. If an attacker can gain remote access and escalate to a privileged account, they can already do whatever they want with the

Iphone iOS 11 QR code scanner provides 'backdoor' exploitable by criminals

1 comment • 5 months ago



Deborah — We just implemented a marketing tool QR code to direct customers to a web page. The scanner or camera in iOS 11 directs one to open a

RDP brute force attacks used to spread LockCrypt ransomware

1 comment • 4 months ago






Dallas H — Here is a technical walk-through on 3 ways to put an end to RDP brute force attempts (beyond disabling it).[https://www.linuxincluded.c...](https://www.linuxincluded.com...)

Russia bans non-compliant VPNs - a blow to privacy and free speech?

1 comment • 4 months ago



LeopoldT — if they do register, does that mean they're essentially a tool by government to track your data? for now, at least those not operating

 Subscribe
  Add Disqus to your site
 Add DisqusAdd
  Privacy

Related Articles



[Hackers crack BlackWallet DNS server, steal US\\$ 400,000](#)

BY [Mark Mayne](#) Jan 16, 2018



[North Korean Monero miner: educational tool or weapon prototype?](#)

BY [Robert Abel](#) Jan 11, 2018



[Report: Expect more website ads to contain hidden cryptominers](#)

BY [Bradley Barth](#) Jan 5, 2018



[The Kosciuszko Institute cyber-security forecasts for 2018](#)

BY The Kosciuszko Institute Jan 5, 2018

Most read on SC

- ['First true' native IPv6 DDoS attack spotted in wild](#)
- [Nation state cyber-attacks on the rise - detect lateral movement quickly](#)
- [Mobile ransomware & banking malware thrive as hackers put focus on mobile](#)
- [RedDrop malware runs up big bills on Android smartphones and spies on users](#)
- [Brute force and dictionary attacks up 400 percent in 2017](#)



SC Media UK arms cyber-security professionals with the in-depth, unbiased business and technical information they need to tackle the countless security challenges they face and establish risk management and compliance postures that underpin overall business strategies.

USER CENTRE

[About Us](#)

[Contact Us](#)

[Advertise](#)

[Partner's
Corner](#)

RESOURCES OTHER

[Issue Archive](#)

[Privacy Policy](#)

[Terms &
Conditions](#)

MORE SC SITES



SC

SCawards

Follow SC Media UK



Copyright © 2017 Haymarket Media, Inc. All Rights Reserved

This material may not be published, broadcast, rewritten or redistributed in any form without prior authorisation.

Your use of this website constitutes acceptance of Haymarket Media's Privacy Policy and Terms & Conditions.